BILL ANALYSIS

Senate Research Center
85R31091 YDB-D

C.S.H.B. 8
By: Capriglione et al. (Nelson)
Business & Commerce
5/18/2017
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Interested parties contend that, as sensitive information is increasingly stored online, there must be a commensurate increase in efforts to protect the data of private citizens from rapidly evolving and sophisticated cyber-attacks. H.B. 8 seeks to minimize Texas' vulnerability to cyber attacks by creating an Information and Analysis Center, providing guidelines for cybersecurity training, requiring risk assessments, and providing other best practice guidance. (Original Author's / Sponsor's Statement of Intent)

C.S.H.B. 8 amends current law relating to cybersecurity for state agency information resources.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Texas Department of Information Resources in SECTION 9 (Section 2054.515, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Authorizes this Act to be cited as the Texas Cybersecurity Act.

SECTION 2. Amends Section 551.089, Government Code, as follows:

> Sec. 551.089. New heading: DELIBERATION REGARDING SECURITY DEVICES OR SECURITY AUDITS; CLOSED MEETING. Provides that this chapter (Open Meetings) does not require a governmental body, rather than the governing board of the Texas Department of Information Resources (DIR), to conduct an open meeting to make certain deliberations.

SECTION 3. Amends Section 552.139, Government Code, by adding Subsection (d), as follows:

> (d) Requires a state agency, when posting a contract on an Internet website as required by Section 2261.253 (Required Posting of Certain Contracts; Enhanced Contract and Performance Monitoring), to redact information made confidential by this section (Exception: Confidentiality of Government Information Related to Security or Infrastructure Issues for Computers) or excepted from public disclosure by this section. Provides that a redaction under this subsection does not except information from the requirements of Section 552.021 (Availability of Public Information).

SECTION 4. Amends Subchapter C, Chapter 2054, Government Code, by adding Section 2054.0594, as follows:

> Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS CENTER. (a) Requires DIR to establish an information sharing and analysis center to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies.
>
> (b) Requires DIR to appoint persons from appropriate state agencies to serve as representatives to the information sharing and analysis center.

(c) Requires DIR, using funds other than funds appropriated to DIR in a general appropriations act, to provide administrative support to the information sharing and analysis center.

SECTION 5. Amends Sections 2054.077(b) and (e), Government Code, as follows:

(b) Authorizes the information resources manager of a state agency to prepare or have prepared a certain report relating to the vulnerability of certain electronic equipment of the agency.

(e) Requires a state agency, separate from the executive summary described by Subsection (b), to prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. Deletes existing text specifying a state agency whose information resources manager has prepared or has had prepared a vulnerability report is required to provide a certain summary.

SECTION 6. Amends Section 2054.1125(b), Government Code, as follows:

(b) Requires a state agency that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law to, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information:

(1) comply with the notification requirements of Section 521.053 (Notification Required Following Breach of Security of Computerized Data), Business & Commerce Code, to the same extent as a person who conducts business in this state; and

(2) not later than 48 hours after the discovery of the breach, suspected breach, or unauthorized exposure, notify DIR, including the chief information security officer and the state cybersecurity coordinator or, if the breach, suspected breach, or unauthorized exposure involves election data, the secretary of state (SOS).

Makes a conforming change.

SECTION 7. Amends Section 2054.133, Government Code, by adding Subsections (b-1), (b-2), and (b-3), as follows:

(b-1) Requires the executive head and information security officer of each state agency to annually review and approve in writing the agency's information security plan and strategies for addressing the agency's information resources systems that are at highest risk for security breaches. Requires that the plan at a minimum include solutions that isolate and segment sensitive information and maintain architecturally sound and secured separation among networks. Requires the highest ranking information security employee for the agency, if a state agency does not have an information security officer, to review and approve the plan and strategies. Provides that the executive head retains full responsibility for the agency's information security and any risks to that security.

(b-2) Requires each state agency to include in the agency's information security plan the actions the agency is taking to incorporate into the plan the core functions of "identify, protect, detect, respond, and recover" as recommended in the "Framework for Improving Critical Infrastructure Cybersecurity" of the United States Department of Commerce National Institute of Standards and Technology. Requires the agency to, at a minimum, identify any information the agency requires individuals to provide to the agency or the agency retains that is not necessary for the agency's operations. Authorizes the agency to incorporate the core functions over a period of years.

(b-3) Requires a state agency's information security plan to include appropriate privacy and security standards that, at a minimum, require a vendor who offers cloud computing services or other software, applications, online services, or information technology solutions to any state agency to contractually warrant that data provided by the state to the vendor will be maintained in compliance with all applicable state and federal laws and rules as specified in the applicable scope of work, request for proposal, or other document requirements.

SECTION 8. Amends Section 2054.512, Government Code, as follows:

Sec. 2054.512. New heading: CYBERSECURITY COUNCIL. (a) Requires, rather than authorizes, the state cybersecurity coordinator to establish and lead a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state. Creates this subsection from existing text.

(b) Requires the cybersecurity council to include certain members.

(c) Requires the state cybersecurity coordinator, in appointing representatives from institutions of higher education to the cybersecurity council, to consider appointing members of the Information Technology Council for Higher Education.

(d) Requires the cybersecurity council to provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

SECTION 9. Amends Subchapter N-1, Chapter 2054, Government Code, by adding Section 2054.515, as follows:

Sec. 2054.515. AGENCY INFORMATION SECURITY ASSESSMENT AND REPORT. (a) Requires each state agency, at least once every two years, to conduct an information security assessment of the agency's information resources systems, network systems, digital data storage systems, digital data security measures, and information resources vulnerabilities.

(b) Requires each state agency, not later than December 1 of the year in which a state agency conducts the assessment under Subsection (a), to report the results of the assessment to DIR, the governor, the lieutenant governor, and the speaker of the house of representatives.

(c) Requires DIR, by rule, to establish the requirements for the information security assessment and report required by this section.

SECTION 10. Amends Section 2054.575(a), Government Code, as follows:

(a) Requires a state agency to, with available funds, identify information security issues and develop a plan to prioritize the remediation and mitigation of those issues. Requires the agency to include in the plan certain procedures, approaches, analyses, information, and strategies.

SECTION 11. Amends Section 2059.055(b), Government Code, to change a reference to a state agency to a governmental entity.

SECTION 12. Amends Subtitle B, Title 10, Government Code, by adding Chapter 2061, as follows:

CHAPTER 2061. INDIVIDUAL-IDENTIFYING INFORMATION

Sec. 2061.001. DEFINITIONS. Defines "cybersecurity risk" and "state agency."

Sec. 2061.002. DESTRUCTION AUTHORIZED. (a) Requires a state agency to destroy or arrange for the destruction of information that presents a cybersecurity risk and alone or in conjunction with other information identifies an individual in connection with the agency's networks, computers, software, or data storage if the agency is otherwise prohibited by law from retaining the information for a period of years.

(b) Provides that this section does not apply to a record involving criminal activity or a criminal investigation retained for law enforcement purposes.

(c) Prohibits a state agency from destroying or arranging for the destruction of any election data before the third anniversary of the date the election to which the data pertains is held.

(d) Prohibits a state agency, under any circumstance, from selling certain information.

SECTION 13. Amends Chapter 276, Election Code, by adding Section 276.011, as follows:

Sec. 276.011. ELECTION CYBER ATTACK STUDY. (a) Requires SOS, not later than December 1, 2018, to:

(1) conduct a study regarding cyber attacks on election infrastructure;

(2) prepare a public summary report on the study's findings that does not contain any information the release of which may compromise any election;

(3) prepare a confidential report on specific findings and vulnerabilities that is exempt from disclosure under Chapter 552 (Public Information), Government Code; and

(4) submit to the standing committees of the legislature with jurisdiction over election procedures a copy of the report required under Subdivision (2) and a general compilation of the report required under Subdivision (3) that does not contain any information the release of which may compromise any election.

(b) Requires that the study include:

(1) an investigation of vulnerabilities and risks for a cyber-attack against a county's voting system machines or the list of registered voters;

(2) information on any attempted cyber attack on a county's voting system machines or the list of registered voters; and

(3) recommendations for protecting a county's voting system machines and list of registered voters from a cyber-attack.

(c) Authorizes SOS, using existing resources, to contract with a qualified vendor to conduct the study required by this section.

(d) Provides that this section expires January 1, 2019.

SECTION 14. (a) Requires the lieutenant governor to establish a Senate Select Committee on Cybersecurity and the speaker of the house of representatives to establish a House Select Committee on Cybersecurity to, jointly or separately, study cybersecurity in this state, the information security plans of each state agency, and the risks and vulnerabilities of state agency cybersecurity.

(b) Requires, not later than November 30, 2017, the lieutenant governor to appoint five senators to the Senate Select Committee on Cybersecurity, one of whom is required to be designated as chair, and the speaker of the house of representatives to appoint five state representatives to the House Select Committee on Cybersecurity, one of whom is required to be designated as chair.

(c) Requires that the committees established under this section convene separately at the call of the chair of the respective committees, or jointly at the call of both chairs. Requires the chairs of each committee, in joint meetings, to act as joint chairs.

(d) Requires the committees established under this section, following consideration of the issues listed in Subsection (a) of this section, to jointly adopt recommendations on state cybersecurity and report in writing to the legislature any findings and adopted recommendations not later than January 13, 2019.

(e) Provides that this section expires September 1, 2019.

SECTION 15. (a) Defines "state agency."

(b) Requires DIR, in consultation with the Texas State Library and Archives Commission (TSLAC), to conduct a study on state agency digital data storage and records management practices and the associated costs to this state.

(c) Requires that the study required under this section examine certain practices, costs, policies, solutions, and benefits.

(d) Requires each state agency to participate in the study required by this section and provide appropriate assistance and information to DIR and TSLAC.

(e) Requires DIR, not later than December 1, 2018, to issue a report on the study required under this section and recommendations for reducing state costs and for improving efficiency in digital data storage and records management to the lieutenant governor, the speaker of the house of representatives, and the appropriate standing committees of the house of representatives and the senate.

(f) Provides that this section expires September 1, 2019.

SECTION 16. Provides that the changes in law made by this Act do not apply to the Electric Reliability Council of Texas.

SECTION 17. Effective date: September 1, 2017.